6-11-2009

Don't Bite

University of Dayton, Ohio (url: http://www.udayton.edu/index.php)

Don't Bite

06.11.2009 | Culture and Society

Now and then, an innocuous-looking e-mail arrives in a UD mailbox, asking the user to verify network access by replying to the message or clicking on a Web link and typing in his or her login and password.

Those are not UD systems, and they're not UD messages, said UDit risk management officer Dean Halter. When users take the bait and enter their information, they are putting not only their own data security at risk, but also UD's.

That's why, later this month, UDit will begin a campaign to raise awareness of e-mail "phishing" scams that can compromise data, clog networks and otherwise complicate UDit's work. Part of the campaign will be a campuswide e-mail asking users to submit their logins and passwords.

"We won't be tracking which users 'bite,'" Halter said. "We'll never know who clicks the link. We just want people to be aware of what these things look like so they'll have a heightened awareness of it."

Those who follow the link will be directed to a UDit information page about the risks of Internet and e-mail scams and how to avoid them.

"Phishing" messages — named for scammers' attempts to cast a wide net with their e-mail appeals and hope a few people take the bait — often look legitimate, so it's an innocent enough mistake, Halter said. Plenty of people do.

"We just had one this morning on a student account, and it happens on faculty and staff accounts, too," he said in early June.

The damage has been relatively minimal because UDit's security measures have been able to identify the compromised access points, "but we may not always be so lucky," he said.

"We are now at the point where we must implement stronger measures to reduce the number of lost IDs and passwords," he said. "The threat to the security of UD's information assets is very real when passwords are compromised."

Halter said the campaign's aim is awareness.

"We encourage everyone to talk about these risks," he said. "Awareness is our best defense."

While this effort is focused on e-mail, Halter said, social engineering scams can be employed over the phone, on the Web and in person, so employees should take care to protect their personal information, regardless of the medium.

Employees can contact the IT service desk at 229-3888 or via e-mail to verify the different IT projects under way.